Board of Management

Audit & Assurance Committee

Date of Meeting	**Thursday 14 March 2024**
Paper No.	**AAC3-O**
Agenda Item	**6.1**
Subject of Paper	**Data Protection Officer: Quarterly Report**
FOISA Status	**Disclosable**
Primary Contact	**Dr Sheila Lodge,** **Depute Principal & Chief Operating Officer**
Date of production	**6 March 2024**
Action	**For Noting**

1. Recommendations

The AAC is asked to note the report.

2. Purpose

The purpose of this paper is to provide the AAC with oversight of current levels of data protection compliance at the College.

3. Consultation

The report has been prepared in consultation with Dr Sheila Lodge.

4. Key Insights

4.1 The DPO has provided a data protection gap analysis report (Appendix 1), updated as at March 2024 to illustrate current levels of data protection compliance at the College and the methodology used by the DPO to assess current levels of compliance.

4.2 The report is mapped to the 10 areas of the ICO's accountability framework and these criteria, set by the ICO, are used to measure compliance rates and identify any gaps.

4.3 The report indicates areas where compliance is being met, areas that need improvement or are currently in the process of being addressed, or where there is a non-conformity to be addressed. Progress is under way in implementing controls to mitigate compliance risks and detail of steps being taken is contained within the report.

4.4 The DPO welcomes comment from the AAC on the report.

5. Impact and Implications

5.1 The report highlights areas where proactive work is being carried out to address gaps in data protection compliance. It is essential that the College continues to invest in its data protection compliance programme with the support of senior management.

5.2 There are financial, legal, regulatory and reputational risks associated with non-compliance with data protection law.

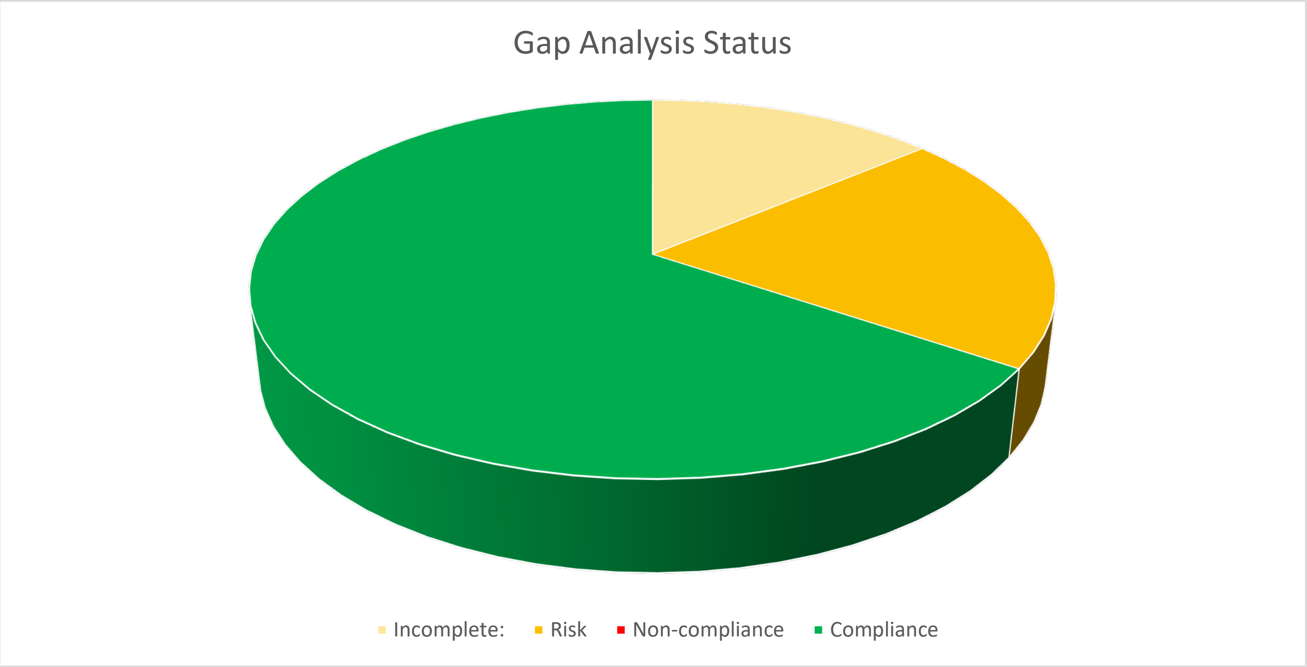
<u>Appendix</u>

Data Protection Gap Analysis (March 2024)

Question title/section		Response	Evidence	GDPR Compliant?	Comments & observations	Interim Update November 2022	Update August 2023	Update March 2024
A	**Governance**							
01	Does the Organisation adopt a structure to manage data protection compliance ensuring there is clear oversight from senior management?	Yes	Yes	Yes	The DPO directly reports to Dr Sheila Lodge, ensuring oversight of data protection risk and management is visible at Senior Management Level	No change	No change	No change
02	Has the board of directors nominated an accountable director?	Yes	Yes	Yes	Dr Sheila Lodge	No change	No change	No change
03	Is DPA/GDPR on each board agenda?	Yes	Yes	Yes	Data Protection features as an agenda item for the AAC and Academic Board.	No change	No change	No change
04	Does the board receive regular audit reports on GDPR compliance?	Yes	Yes	Yes	Yes	No change	No change	No change
05	Does the organisation require a DPO?	Yes	Yes	Yes	Yes.	No change	No change	No change
06	If yes, has the appointment of a DPO been made?	Yes	Yes	Yes	Thorntons Solicitors fulfil this role. (Morgan O'Neill)	Thorntons Solicitors fulfil this role	Thorntons Solicitors fulfil this role	Thorntons Solicitors fulfil this role
07	Is the individual(s) able to discharge their role with independence?	Yes	Yes	Yes	Yes	No change	No change	No change
08	Is the DPO's role adequately supported and provided with the necessary resources to discharge their duties?	Yes	Yes	Yes	Yes	No change	No change	No change
09	Who does the DPO report to?.	Yes	Yes	Yes	Dr Sheila Lodge	No change	No change	No change
10	Is the DPO adequately qualified to undertake the position?	Yes	Yes	Yes	Yes	No change	No change	No change
11	Is there a group established to lead on data protection compliance?	Q.Yes	Q.Yes	Risk	Key business managers have been identified to lead on data protection for departments and faculties. This is in the early stages of development.	This is still in the early stages. More department leads have been engaged in record keeping excercises since the last report but the role of "data protection lead" has not been formalised.	Department Heads/Managers identified to complete the ROPA exercise have been informally assigned as DP Contacts for the College. Business Managers have been identified as contacts for Data Protection matters and engaged by the DPO.	Department Heads/Managers identified to complete the ROPA exercise have been informally assigned as DP Contacts for the College. Business Managers have been identified as contacts for Data Protection matters and engaged by the DPO.
12	If yes, what is the role and remit of this group? Who attends?	Q.Yes	Q.Yes	Risk	The group will meet as a committee of data protection leads. Terms of reference are yet to be agreed.	No change.	No change.	No change.
B	**Policies and Procedures**							
01	Has the organisation adopted policies and procedures pertaining to data protection compliance?	Yes	Yes	Yes	Yes	No change.	No change.	No change.
02	Do these policies and procedures provide staff with the appropriate rules that apply and the processes which must be followed to demonstrate compliance with the law?	Yes	Yes	Yes	Yes	No change.	No change.	No change.
03	Is there a process for reviewing these policies and procedures?	Yes	Yes	Yes	Yes, annually.	No change.	No change.	No change.
04	Is there an approval process for the policies and procedures?	Yes	Yes	Yes	Yes, any material changes are submitted to Sheila Lodge and Michael Cross for approval.	New College Secretary will be included in the approval process.		
05	Are staff fully aware of these policies and procedures (how are they made aware, and how do they know if they are relevant to their role?)	Q.Yes	Q.Yes	Risk	There is some evidence that processes are followed. This is demonstrated via requests for support in relation to data sharing, DPIAs, reporting of data breaches and escalation of data subject rights. More could be done to raise awareness of data protection policies and procedures throught a regular communications strategy.	The DPO is working with collegeagues to improve awareness of the data subject rights process and we have undertaken an audit of the data protection policy suite upon discovery that some out of date policy versions were in circulation.	All Data Protection Policies have been reviewed and updated as necessary, including the data subject rights process. An Appropriate Policy Document and Conlict of interest policy have been drafted to be submitted for approval. The records retention policy is under review with a deadline of September 2023. There is some evidence of awareness of the College Data Protection Policies however this has not been tested. The DPO intends to launch a data protection health check for departments and faculties to assess whether policies and procedures are being adhered to (attached). Note that this health check was paused due to priority being given to the completion of Department Records of Processing Activities.	All Data Protection Policies have been reviewed and updated as necessary, including the data subject rights process. The records retention policy and procedure has been updated and submitted for approval. The data protection policy has been updated and submitted for approval. The data breach policy and procedure is currently being revised and will be shared with IT and COO for input prior to seeking approval. There is some evidence of awareness of the College Data Protection Policies however this has not been tested. The DPO intends to assess understanding via a data protection health check for departments and faculties commencinfg March 2024, to assess whether policies and procedures are being adhered to.
06	Do these policies and procedures adopt a data protection by design and by default approach across the organisations?	Yes	Yes	Yes	Yes	No change.	No change.	No change.
C	**Training and Awareness**							
01	Do you have an all-staff data protection training programme?	Yes	Yes	Yes	Yes, however the current module is out of date. A new module was procured in August 2022 work is being undertaken by the L& Team and DPO to finalise the training for publication. This training will be mandatory. Supplementary DPO-led training was delivered in 2021 while a new training provider was identified.	More progress has been made in the tailoring of the College data protection module. The DPO worked with the L&D Team to finalise edits to the module at the end of October and we expect the module to be available early 2023.	The DPO has worked with the OD team to design a new data protection e-learning module tailored for the College. This module launched in January 2023. Completin rates are below expectations and this mandatory training is being reclaunched on 31/8/23 with a requirement for all staff to compelte it by 31/10/23. Completion rates will be monitored by the DPO and OD.	Completion rates as at March 2024: 847 out of 1141 staff members have completed mandatory data protection training. A further reminder will be issued to all staff in March 2024. The DPO will survey some departments and facullties on completion rates during March - June 2024. The training will be relaunched in August 2024 with a module refresh and all staff will ben required to complete within 3-months.
02	Is there a process for induction data protection training?	Yes	Yes	Yes	All new employees are required to undertake mandatory data protection training.	No change.	No change.	No change.
03	Is there refresher data protection training (how frequently)?	Yes	Yes	Yes	Data protection training is not repeated frequently. The new training module will be completed annually.	No change. However annual training shall commence upon publication of the new training module.	The e-learning module has been calendared as an annual mandatory training exercise.	The e-learning module has been calendared as an annual mandatory training exercise. A refreshed module will be launched in August 2023.
04	Are specialised roles and/ or function, or are that are responsible for large-scale processing or the processing of special category personal data provided with additional training?	Yes	Yes	Yes	Some tailored data protection training has been delivered to the security team and marketing team. The DPO is addressing additional training requirements and bespoke training is available on request.	No change.	The e-learning module includes a tailored section relating to the processing of personal data.	The e-learning module includes a tailored section relating to the processing of personal data.
05	Does the DPO receive training and CPD to aide their ongoing development and knowledge of data protection?	Yes	Yes	Yes	Yes - via Thorntons LLP	No change.	No change.	No change.
06	Is there a business-wide awareness programme?	Q.Yes	Q.Yes	Risk	Occasional communications are issued and a data protection review of departments and faculties is underway.	No change.	Occasional communications are issued. Since the date of the last report a Data Protection SharePoint site has been created where resources can be accessed.	Focussed communications relating to policy and procedure updates are scheduled.
07	How frequently are staff provided with awareness of data protection within the business (what are the contents of these communications/ are they event led or systematic?)?	Q.Yes	Q.Yes	Risk	A more frequent awareness raising comms plan is recommended.	No change.	See above.	See above.
D	**Individual Rights**							
01	Is there acceptable means/ systems in place that allow individuals to exercise their rights e.g. Privacy Notice notifying the individual how to exercise their right/ portal for raising requests/ dedicated helpline, etc.	Yes	Yes	Yes	This information is clearly communicated via the College privacy notices availabe on its website.	No change.	No change.	No change.
02	Does the business inform individuals about their rights?	Yes	Yes	Yes	Yes, via privacy information	No change.	No change.	No change.
03	Do staff know how to handle requests from individuals	Yes	Yes	Yes	There is an escalation process whereby requests received are escalated to the data protection mailbox. The majority of requests are received directly to the DPO via the designated mailbox.	No change.	No change.	No change.
04	Does the business have a log for all data subject engagements pertaining to the exercising of their rights?	Yes	Yes	Yes	Yes	No change.	No change.	No change.

05	Does the business ensure they fulfil all requests in a timely manner?	Yes	Yes	Yes	There are no recorded instances of failure to comply with a requests within the specified staturoty timeframe.	No change.	No change.	No change.
06	Does the business have a system for reporting all requests internally i.e. notifying senior staff of volume and nature of requests?	Yes	Yes	Yes	Requests are direct to dpo@cityofglasgowcollege.ac.uk	No change.	No change.	No change.
07	Does the business have a system for managing complex requests?	Yes	Yes	Yes	These are currently led by the DPO. The process is under review to assess whether efficiencies can be made.	No change.	No change.	No change.
E	**Transparency**							
01	Does the business have the appropriate Transparency notices?	Yes	Yes	Yes				Annual review in progress
02	Is there a process for managing and updating transparency notices?	Yes	Yes	Yes	Yes - annual review	No change.	No change.	Annual review in progress
03	Are the privacy easy to access?	Yes	Yes	Yes	Available on the College website and intranet.	No change.	No change.	No change.
04	Are the privacy notices clear, intelligible and use plain language?	Yes	Yes	Yes		No change.	No change.	No change.
05	Is there appropriate information relating to automated decision making [if applicable].	Select	Select	Incomplete	N/A	No change.	No change.	No change.
06	Are relevant staff members able to demonstrate knowledge on how to access these privacy notices?	Yes	Yes	Yes	Yes, the privacy notice is widely accessible	No change.	No change.	No change.
07	Are relevant staff members able to summarise details of the consent within the privacy notices?	Select	Select	Incomplete	N/A - as consent is used in limited circumstances this is not a high risk area for the College. Consent has been covered in marketing training, where it is likely to be most relevant.	N/A	N/A	N/A
08	Is there suitable measures of transparency in place for the purposes of processing child data (if applicable)?	Select	Select	Incomplete	N/A	N/A	N/A	N/A
F	**Lawfulness of Processing and relevant records of Processing**							
01	Has the business carried out a comprehensive data mapping exercise?	Q.Yes	Q.Yes	Risk	A data mapping exercise had been carries out and a review is currently under way to ensure the data has been mapped accurately.	The data mapping exercise is ongoing. Since the date of the last report the DPO has assisted 10 departments with the progression of their ROPAs to ensure compliance with Art 30 of UK GDPR.	Phase 1 of the data mapping exercise concluded on 30th June 2023 with 10 core Departments in the College completing their ROPAs with the support of the DPO. The ROPAs will be subject to a review in 6-months. While significant progress has been made with Departments, this action remains amber as Phase 2 of this project will require Faculties to refresh and re-draft their ROPAs with the support of the DPO and business managers. This will commence in September 2023	Phase 2 is underway with ROPAs being reviewed and revalidated across heavy and high risk processing areas including student records and student support. Faculty ROPA work is in progress. A new ROPA has been drafted with support of faculty business managers.
02	Does the business have a formal, comprehensive and completed Record of Processing Activities (ROPA)?	Q.Yes	Q.Yes	Risk	As above, a ROPA for each department and faculty exists and these have been revieed by the DPP and are being distributed to departments and facultioe for validation to ensure they are accurate, up to date and compliant with Art 30 of GDPR.	No change.	As above	As above
03	Does the business have a formal process for relevant stakeholders to manage, maintain and update aspects of the ROPA relevant to them?	Yes	Yes	Yes	Not currently, however the identification of a person responsible for the maintenance of the ROPA is a step in the data protection review process.	Progress is being made and the DPO is working with department and faculty representatives across the College but the role is still to be formalised.	Heads of Departments/Managers are identified on each ROPA and will be responsible for maintaining the ROPA. Completed ROPAs are scheduled for review in 6-months as part of an ongoing monitoring process to be coordinated by the DPO with support from Compliance Auditor and PMO.	As noted above - ROPA owners are being asked to review their ROPAs, commencing with the highest risk business areas.
04	Is there a process that has identified Information Asset Owners?	Yes	Yes	Yes	Documented on ROPA (validation in progress)	Documented on ROPA (validation in progress)	Documented on ROPA (validation in progress)	Yes
05	Has the business appropriately identified the necessary lawful bases for processing personal data?	Yes	Yes	Yes		No change.	No change.	No change.
06	Where applicable, are these lawful bases justified?	Yes	Yes	Yes		No change.	No change.	No change.
07	Does the business rely on legitimate interest? If so, have legitimate interest assessments been carried out?	Yes	Yes	Yes	Legitimate interest is relied upon for certain procesing activities but an LIA has not been completed in all cases. However, where an LIA is required, the DPO would initiate this.	No change.	This has been amended to green as awareness is raised via training and policy. This will be reviewed and tested via the Health Check questionnaire.	Health Check questionnaire exercise will commence in March 2024.
08	Does the business rely on consent?	Yes	Yes	Yes	In limited circumstances.	No change.	No change.	No change.
09	Is so, is there a procedure for recording, managing and maintaining consents?	Yes	Yes	Yes	Yes	No change.	No change.	No change.
10	Does the business process any special category data?	Yes	Yes	Yes	Yes	No change.	No change.	No change.
11	If so, is there appropriate recorded information regarding valid exceptions in place?	Yes	Yes	Yes	Yes	No change.	No change.	No change.
G	**Contract and Data Sharing**							
01	Is there a record of data sharing in place?	Q.Yes	Q.Yes	Risk	This is being reviewed on a department and faculty basis during each ROPA review. Further, the DPO is workignwith the procurement team to review processing arrangements with third party suppliers and ensure valid data processign agreements are in place.	No change - this exercise is ongoing and is built in to the ROPA review process.	As of June 2023, the College has a clearer understanding of data sharing activities undertaken by departments but there is still some investigation required to ensure these arrangements are clearly documented and understood. This will be addressed via the health check.	The DPO has been compiling a list of suppliers during Phase 2 of the ROPA exercise to review the contractual position with the Procurement Team duriing monthly meetings (next meeting 21/3/24)
02	Are there valid contract in place for data sharing, where it is relevant to do so?	Q.Yes	Q.Yes	Risk	There are data processing and sharing contracts in place with third parties. A comprehensive review is under way to ensure there are no gaps.	No change - this exercise is ongoing and is built in to the ROPA review process.	As above.	As above.
03	Are there measures in place for handling restricted transfers?	Yes	Yes	Yes	The DPO and procurement team have relevant contract templates in place.	No change.	No change.	No change.
04	Does the business have the relevant data protection contractual provisions in place with suppliers/ customers/ clients?	Q.Yes	Q.Yes	Risk	There are data processing and sharing contracts in place with third parties. A comprehensive review is under way to ensure there are no gaps.	No change - this exercise is ongoing and is built in to the ROPA review process.	As above.	The Procurement Team requires a GDPR Assessment to be completed ahead of a tender or PO request via PECOS and refers these to the DPO. This is assisting in identifying suppliers which are data processors and ensuring that DPAs and DSAs are in place.
05	Is there a process in place to carry our due diligence?	Q.Yes	Q.Yes	Risk	This forms part of the procurement process. There is currently a gap where lower value service providers are concerned. The DPO has supported with completion of DPIAs and putting in place data processing agreements but the establishmnet of a more robust supplier management process would reduce data protection risk and improve compliance.	No change.	No change.	As above - improvements have been made as a result of the GDPR Assessment requirement above.
06	Is there a process in place for reviewing contracts?	Q.Yes	Q.Yes	Risk	Yes, an exercise is under way to review this as part of the ROPA validation, but this could be better established and departments/faculties will be required to take responsibility for supplier contracts/relationships, seeking advice from the DPO as necessary.	No change - this exercise is ongoing and is built in to the ROPA review process.	No change - this exercise is ongoing and is built in to the ROPA review process.	No change - this exercise is ongoing and is built in to the ROPA review process.
07	Have all international data transfers been identified?	Q.Yes	Q.Yes	Risk	This is being considered as part of the ROPA review.	No change - this exercise is ongoing and is built in to the ROPA review process.	No change - this exercise is ongoing and is built in to the ROPA review process.	No change - this exercise is ongoing and is built in to the ROPA review process.
08	Are there the appropriate safeguards in place?	Yes	Yes	Yes	Where international data transfers have been identified, safeguards are in place.	No change.	No change.	No change.
H	**Information Security and Record Management**							
01	Is there an information security policy?	Select	Select	Incomplete				
02	Are all relevant devices encrypted?	Yes	Yes	Yes				

03	Are databases encrypted?	Select	Select	Incomplete	It is understood that IT controls are assessed via a separate audit and assurance process at CoGC and this review has not progressed on this basis.			
04	Is pseudonymisation deployed?	Select	Select	Incomplete				
05	Are emails encrypted?	Yes	Yes	Yes				
06	Is there regular external network penetration testing?	Select	Select	Incomplete				
07	Is there regular internal network penetration testing?	Select	Select	Incomplete				
08	Are websites/applications regularly security tested?	Select	Select	Incomplete				
09	Does the information security policy reference security of data subjects?	Select	Select	Incomplete				
10	Are there any certification standards adopted? E.g. cyber essentials, ISO 27001, etc.?	Select	Select	Incomplete				
11	Are physical records stored securely?	Q.Yes	Q.Yes	Risk	Generally, yes. However, we are aware that some records are held in store rooms which may not be secure and data may not be adequately organised or tagged.	No change.	No change.	No change.
12	Are there procedures in place to reduce the amount of information and to only retain what is necessary?	Q.Yes	Q.Yes	Risk	There is no robust process in place to determine retention requirements.	No change.	There is no robust process in place to determine retention requirements at present but this has been addressed with 10 departments via the ROPA/data mapping exercise. Data retention schedules require review and compliance should be monitored. This will be addressed via the health check and other project work being undertaken across the College relating to Archiving and Retention.	The data retention polocy and procedure was revised and is awaiting committee approval. The policy will be relaunched and the DPO will advise departments and faculties on their retention obligations.
13	Is there a retention schedule in place?	Q.Yes	Q.Yes	Risk	There is a records retention policy but the DPO does not have sufficient evidence of this being routine practice across the College. This is being addressed as part of the ROPA review.	No change - this exercise is ongoing and is built in to the ROPA review process.	As above.	As above.
14	Is it actively managed ensuring that out of date data is destroyed securely?	Q.Yes	Q.Yes	Risk	This is being reviewed to be updated and aligned with the ROPA.	No change - this exercise is ongoing and is built in to the ROPA review process.	As above.	As above.
15	Is there confidential waste processes in place?	Yes	Yes	Yes	The College operates confidential disposal practices.	No change	No change.	No change.
I	**Risks and Data Protection Impact Assessments (DPIA)**							
1	Does the business have a risk register which identifies data protection risks?	Yes	Yes	Yes		No change.	No change.	No change.
2	Where applicable, are these risks remediated with an action plan?	Yes	Yes	Yes		No change.	No change.	No change.
3	Are these risks managed by an accountable business owner?	Yes	Yes	Yes		No change.	No change.	No change.
4	Are measures in place that adopt the use of DPIA's?	Q.Yes	Q.Yes	Risk	This is built into the procurement process. Outside of the procurement process, there is a risk that DPIAs are not consistently initiated to document new high risk processing activities.	This is built into the procurement process. The DPO has supported with the completion of 2 DPIAs in 2022. There is a risk that DPIAs are not consistently initiated to document new high risk processing activities.	The DPO has supported colleagues in the completion of 6 DPIAs. This has created an opportunity to raise awareness and general understanding of the requirements to complete a DPIA and the process. Since the date of the last report, a number of DPIAs have been reviewed by the ethics committee. This indicates that awareness is improving	No change.
5	Is there a policy/ procedure that identifies when DPIA's are necessary and how to complete them properly?	Yes	Yes	Yes	A template is available with screening questions and this requiredment has been commnication via training and the data protection policy. We have seen an increase in completion of DPIAs. The DPO retains a record of DPIAs completed.	No change.	No change.	No change.
6	Are there processes in place to ensure high-risks identified within the DPIA's are communicated with senior management?	Yes	Yes	Yes	Yes, the DPO will escalate as necessary.	No change.	No change.	No change.
J	**Breach Response and Monitoring**							
01	Is there an active Data Breach Policy in place?	Yes	Yes	Yes		No change.	No change.	The data breach policy and procedure is under review and the DPO is consulting with IT to improve the process for escalating and responding to data breach reports.
02	Are staff familiar with this policy?	Yes	Yes	Yes	Data breaches are reported promptly by staff.	No change.	No change.	No change.
03	Are there procedures in place that aide the business in detecting, managing and appropriately recording data events, incidents and/ or breaches?	Yes	Yes	Yes	Yes, reporting forms and logs are retained.	No change.	No change.	No change.
04	Are there procedures in place for notifying affected individuals should their be a high-risk to their data protection rights and freedoms?	Yes	Yes	Yes	Yes, the DPO would notify as necessary.	No change.	No change.	No change.
05	Is there an internal audit programme?	Yes	Yes	Yes		No change.	No change.	No change.
06	When was the audit last completed?	Select	Select	Incomplete		No change.	No change.	No change.
07	Have all advisory notes been completed or have an associated remediation plan which are providing active progress?	Yes	Yes	Yes		No change.	No change.	No change.
08	Are management/ executive providing with regular updates/ progress/ issues/ risks relating to data protection compliance?	Yes	Yes	Yes		No change.	No change.	No change.


Gap Analysis Status
Incomplete:
Risk
Non-compliance
Compliance